PCT/JP99/04328

09/787029

10.08.99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　９月２４日

出願番号
Application Number: 平成１０年特許願第２７０１４９号

出願人
Applicant (s): 科学技術振興事業団

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年　８月２７日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０５９８８８

【書類名】　特許願
【整理番号】　PJST1567
【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願
【提出日】　平成10年 9月24日
【あて先】　特許庁長官　殿
【発明の名称】　量子暗号通信システム
【請求項の数】　10
【発明者】
　【住所又は居所】　東京都豊島区目白１－５－１　学習院大学理学部物理学科内
　【氏名】　平野　琢也
【特許出願人】
　【識別番号】　396020800
　【氏名又は名称】　科学技術振興事業団
【代理人】
　【識別番号】　100082876
　【弁理士】
　【氏名又は名称】　平山　一幸
　【電話番号】　03-3352-1808
【選任した代理人】
　【識別番号】　100069958
　【弁理士】
　【氏名又は名称】　海津　保三
【手数料の表示】
　【予納台帳番号】　031727
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　量子暗号通信システム

【特許請求の範囲】

【請求項１】　光信号を用いる量子暗号通信において、

盗聴の操作によって生じる信号光の振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする、量子暗号通信システム。

【請求項２】　前記量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で上記参照信号と上記伝送信号とに位相差を付与し、これらの２信号を受信側で重ね合わせて得られる相互に逆位相の関係にある２つの出力光の差を求め、上記伝送信号の量子状態の揺らぎに依存した上記出力光の差の頻度分布に基づいて送信側と受信側との秘密鍵を共有するとともに、上記伝送信号の量子状態の揺らぎを直接測定するようにしたことを特徴とする、請求項１に記載の量子暗号通信システム。

【請求項３】　前記出力光の差の信号に正負それぞれにしきい値を設定し、このしきい値を基準にして前記伝送信号の状態を判別することを特徴とする、請求項１又は２に記載の量子暗号通信システム。

【請求項４】　前記位相差の付与がランダムな位相変調の他に予め定めた位相変調を与えることによって外的な要因による前記参照信号と前記伝送信号との光路差の変動を補正することを特徴とする、請求項１乃至３の何れかに記載の量子暗号通信システム。

【請求項５】　前記参照信号と前記伝送信号とを時間及び偏光状態で分離して同一の経路を伝送したことを特徴とする、請求項１乃至４の何れかに記載の量子暗号通信システム。

【請求項６】　光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、上記伝送信号に位相変調を与える位相変調手段と、この伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、上記参照信号に位相変調を与える位相変調手段とを備え、

出証特平１１－３０５９８８８

上記位相変調した微弱な伝送信号と上記位相変調した強度の強い参照信号とを重ね合わせ出力する第２のビームスプリッターと、この第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、この第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

【請求項７】　光源からの光を伝送信号と参照信号とに分割するビームスプリッターと、上記伝送信号を一方の長い経路を通し偏光する第１の偏光素子と、この伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、この伝送信号に所定の位相変調を与える第１の位相変調手段と、他方の短い経路に通した強度の強い上記参照信号と上記伝送信号とを同一光軸上に戻す第１の偏光ビームスプリッターとを備え、

受信側にて一本の光ファイバーを伝送してきた上記伝送信号及び上記参照信号を分離する第２の偏光ビームスプリッターと、この分離した伝送信号を一方の短い経路に通し位相変調を与える第２の位相変調手段と、上記分離した参照信号を他方の長い経路に通し偏光する第２の偏光素子とを有しており、

時間及び偏光状態が一致した上記伝送信号と上記参照信号とを重ね合わせ出力する無偏向ビームスプリッターと、この無偏向ビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、この第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有する、量子暗号通信システム。

【請求項８】　前記光ファイバーの出力側に前記参照信号の偏光の乱れを補正する第３の偏光素子を設けたことを特徴とする、請求項７に記載の量子暗号通信システム。

【請求項９】　前記２つの出力光をフォトダイオードで電気変換することを特徴とする、請求項１乃至８の何れかに記載の量子暗号通信システム。

【請求項１０】　光の波長が６００ｎｍ～９００ｎｍのときシリコンフォトダイオードを用い、光の波長が１０００ｎｍ～１５００ｎｍのときＩｎＧａＡｓフォトダイオードを用いることを特徴とする、請求項１乃至９の何れかに記載の量子暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は通信の安全性を確保するための秘密鍵の配布に利用し、特に伝送信号の量子力学的な状態を測定し、実質的に高い量子効率で伝送信号の検出をするための量子暗号通信システムに関する。

【０００２】

【従来の技術】

通信の安全性を確保するための従来の暗号技術には、正規の通信者のみが知っている共通の秘密鍵を用いる秘密鍵暗号方式と、秘密鍵と公開鍵という一対の鍵を用いる公開鍵暗号方式とがある。

公開鍵暗号方式の暗号は、その秘蔵性を、例えば非常に大きな正数の因数分解が計算困難であるといったことに依っているが、計算機の性能の進歩やネットワークを使った分散処理の発達等によりその安全性は必ずしも万全とはいえない。

【０００３】

これに対して、正規の通信者のみが知っている秘密鍵を送り手と受け手のみで共有することができれば絶対的に安全な通信が可能になる。このような中で秘密鍵の配布方法の秘蔵性を量子力学の原理にもとめる通信方法である量子暗号が提案されている（Ｊ．Ｃｒｙｐｔｏｌｏｇｙ、５、３－２８（１９９２）Ｃ．Ｈ．Ｂｅｎｎｅｔｔ　ｅｔａｌ）。

【０００４】

量子力学の原理によれば、測定行為は必然的に被測定対象に擾乱を与えるので、盗聴者による盗聴の試みは必ず信号に変化を与える。

したがって、信号の変化を監視することにより盗聴者の存在を暴くことができる。つまり、量子暗号を用いると距離的に離れた２点間で秘蔵性の非常に高い秘密鍵を共有することができる。従来の量子暗号は伝送信号の担い手として光を用い、かつ、光の検出に光子計数法を用いている。光子計数法とは１個以上の光子が検出器に入射したとき、ある確率（量子効率という）で電気パルスが発生する光の検出方法である。

【０００５】

【発明が解決しようとする課題】

しかしながら、このような従来の方法では、光の検出に光子計数法を用いているため、そのことに起因する原理的及び技術的な解決すべき課題がある。

まず、原理的な課題は、伝送された後の信号の量子力学的な状態を調べることが出来ないので、盗聴者が量子非破壊測定等の高度な手段をとった場合、それを検知することができない。すなわち、盗聴者が光子数の情報を信号の光子数に変化を与えずに読み出すことが可能なので（測定の影響は位相の変化に現れる）、伝送後の光子数のみを測定していても盗聴に気がつかないことになる。

【０００６】

さらに技術的な課題として、光通信で通常用いられる１．３μｍや１．５μｍの光に対して、高い量子効率を有する検出器が現存しないことがある。検出の際の損失はデータの転送レートを低下させるだけでなく、原理的には盗聴者による盗聴の試みと区別できない。

【０００７】

そこで、本発明は伝送信号の量子力学的な状態の測定が可能になるとともに、実質的に高い量子効率で伝送信号の検出が可能な量子暗号通信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記目的を達成するために、本発明の量子暗号通信システムのうち請求項１記載の発明は、光信号を用いる量子暗号通信において、盗聴の操作によって生じる信号光の振幅と位相とで規定される量子力学的な確率分布の変化に基づいて盗聴を検出することを特徴とする。

また請求項２記載の発明は、量子暗号通信において、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号と伝送信号とに位相差を付与し、これらの２信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある２つの出力光の差を求め、伝送信号の量子状態の揺らぎに依存した出力光の差の頻度分布に基づいて送信側と

受信側との秘密鍵を共有するとともに、伝送信号の量子状態の揺らぎを直接測定することを特徴とするとするものである。

【０００９】

さらに請求項３記載の発明は、出力光の差の信号に正負それぞれにしきい値を設定し、このしきい値を基準にして伝送信号の状態を判別することを特徴としている。

また請求項４記載の発明は、位相差の付与がランダムな位相変調の他に予め定めた位相変調を与えることによって外的な要因による参照信号と伝送信号との光路差の変動を補正することを特徴とするものである。

さらに請求項５記載の発明は、参照信号と伝送信号とを時間及び偏光状態で分離して同一の経路を伝送したことを特徴とする。

【００１０】

また請求項６記載の発明は、光源からの光を伝送信号と参照信号とに分割する第１のビームスプリッターと、伝送信号に位相変調を与える位相変調手段と、伝送信号を量子力学的な状態変化で検出できる微弱な信号にする光減衰器と、参照信号に位相変調を与える位相変調手段とを備え、位相変調した微弱な伝送信号と位相変調した強度の強い参照信号とを重ね合わせ出力する第２のビームスプリッターと、第２のビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

【００１１】

さらに請求項７記載の発明は、光源からの光を伝送信号と参照信号とに分割するビームスプリッターと、伝送信号を一方の長い経路を通し偏光する第１の偏光素子と、伝送信号を量子力学的な状態で検出できる微弱な信号にする光減衰器と、伝送信号に所定の位相変調を与える第１の位相変調手段と、他方の短い経路に通した強度の強い参照信号と伝送信号とを同一光軸上に戻す第１の偏光ビームスプリッターとを備え、一本の光ファイバーを伝送してきた伝送信号及び参照信号を分離する第２の偏光ビームスプリッターと、分離した伝送信号を一方の短い経路に通し位相変調を与える第２の位相変調手段と、分離した参照信号を他方の長

い経路に通し偏光する第２の偏光素子とを有しており、時間及び偏光状態が一致した伝送信号と参照信号とを重ね合わせ出力する無偏向ビームスプリッターと、無偏向ビームスプリッターの２つの出力光を電気変換する第１及び第２の光電変換素子と、第１及び第２の光電変換素子の逆位相の差信号を増幅して電圧を出力する増幅器とを有するものである。

【００１２】

また請求項８記載の発明は、上記構成に加え、光ファイバーの出力側に参照信号の偏光の乱れを補正する第３の偏光素子を設けたことを特徴とする。

さらに請求項９記載の発明は、２つの出力光をフォトダイオードで電気変換することを特徴とする。

また請求項１０記載の発明は、光の波長が６００ｎｍ～９００ｎｍのときシリコンフォトダイオードを用い、光の波長が１０００ｎｍ～１５００ｎｍのときＩｎＧａＡｓフォトダイオードを用いることを特徴とするものである。

【００１３】

このような構成により、請求項１記載の発明では、伝送信号の量子状態をモニターすることにより、従来は困難であった量子非破壊測定のような高度な盗聴の検出ができる。

また請求項２記載の発明では、参照信号の強度が強いことにより、理論的な上限に近い効率で伝送信号を検出することができる。

さらに請求項３記載の発明では、しきい値を設定することにより、伝送信号の強度に応じて実効的な検出効率と誤り率とを自由に選ぶことが出来る。

また請求項４記載の発明では、ランダムな位相変調と予め定めた位相変調を与えることにより、光路差の変動の補正と量子状態の測定とを量子暗号と同時に行うことができる。

さらに請求項５記載の発明では、伝送路として１本の光ファイバーで伝送するので、長距離の量子暗号通信システムが提供できる。

【００１４】

また請求項６記載の発明では、送信側からの光信号を強度の強い参照信号と量子力学的状態変化を検出できる微弱な伝送信号とに分離し、送信過程で参照信号

と伝送信号とに位相差を付与し、この２信号を受信側で重ね合わせ、得られる相互に逆位相の関係にある２つの出力の差を求め、伝送信号の量子状態の揺らぎに依存した出力の差の頻度分布に基づいて送信側と受信側の秘密鍵を共有し、伝送信号の量子状態の揺らぎを測定する。したがって、高効率の検出ができるとともに信号光の量子状態を測定することができる。

【００１５】

さらに請求項７記載の発明では、伝送信号と参照信号とが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、長距離の量子暗号伝送であっても２つの光の相対的な光路差の変動を小さくすることができる。

また請求項８記載の発明では、光ファイバー伝送中の偏光の乱れを強度の強い参照信号で行うので、偏光の乱れを効果的に補正することができる。

さらに請求項９及び１０記載の発明では、高い量子効率かつ十分なＳ／Ｎ比で信号の測定ができる。

【００１６】

【発明の実施の形態】

以下、図面に示した実施形態に基づいて本発明を詳細に説明する。

図１は本発明による量子暗号通信システムの第１の実施形態の模式図である。図１を参照して本実施形態を説明すると、この量子暗号通信システムは送信者の装置１０、伝送路１４，１６及び受信者の装置１２からなり、送信者の装置１０は、レーザー光源１と、ビームスプリッター２と、鏡３と、光減衰器４とを備えている。

レーザー光源１から出た光は、ビームスプリッター２で参照光Ｌと信号光Ｓとに分割される。信号光Ｓを反射する鏡３は光の波長程度の微少な距離の移動が可能で信号光Ｓの位相を変化させる。

【００１７】

信号光Ｓは光減衰器４により強度が減少し、典型的な強度が光子１個程度となるようにし、量子力学的な状態変化を検出できる微弱な信号にしている。

参照光Ｌの典型的な強度は光子１千万個程度であり、信号光Ｓと参照光Ｌの強

度は著しく異なるように調節されている。

したがって、参照光Ｌの光の強度が信号光Ｓの光の強度よりも著しく大きいため、高効率の検出が可能になるとともに、信号光Ｓの量子状態の測定が可能になる。

【００１８】

受信者の装置１２は、光の波長程度の微少な距離の移動が可能な鏡５と、光の透過率と反射率とが等しいビームスプリッター６と、フォトダイオード７ａ，７ｂと、増幅器及び電圧測定器８とを備えている。

受信者は鏡５を移動することにより参照光Ｌと信号光Ｓとの相対的な位相差を変化させたあと、ビームスプリッター６上で２つの光を重ね合わせる。ビームスプリッター６からの２つの出力光はフォトダイオード７ａ，７ｂによりそれぞれ電気信号に変換する。さらに、その差信号を増幅し電圧を測定する。増幅器８にはチャージセンシティブアンプを用い、その典型的な利得は３０Ｖ／ｐＣ（ピコクーロン）なので、差信号に１万個の電子が含まれているときの出力電圧は５０ｍＶ程度となる。

【００１９】

フォトダイオードとしては波長が６００～９００ｎｍの光に対してはＳｉを、波長が１０００～１５００ｎｍの光に対してはＩｎＧａＡｓを使用すれば量子効率９０％以上、最適な場合では９９％以上の量子効率を実現できる。つまり、最適な場合、参照光Ｌの強度が強いということから例えば１万個の光子を９９００個以上の電子に変換し、その電子数を十分にＳ／Ｎ比で測定することが可能である。

【００２０】

次に受信者の信号処理について説明する。以下の説明では簡単のためフォトダイオードの量子効率を１００％とし、また増幅器の雑音は無視できるとした。

図１を参照して、信号光Ｓと参照光Ｌはビームスプリッター２で分割された後、別の経路を通りビームスプリッター６上で重なり合うので、２つの経路の光路差により干渉を起こす。

ただし、２つの光の強度が著しく異なるので干渉稿の明瞭度は低い。

【００２１】

図２は信号光の量子状態の揺らぎを考慮しない場合の受信者側の測定信号の模式図であり、（ａ）は参照光と信号光の経路の相対的な光路差とフォトダイオードに入射する光子数との関係図であり、挿入図は光路差がゼロ付近の拡大図である。図２（ｂ）は参照光と信号光との差信号を示す図である。

【００２２】

図２（ａ）に示すように、ビームスプリッター６は信号光Ｓがないときに参照光Ｌを１対１に分割するよう調整するので、２つのフォトダイオード７ａ，７ｂに入射する光子数は共に参照光Ｌの光子数ｎ０ の半分程度である。それを中心として２つの経路の相対的な光路差に応じて微少な干渉稿が現れる。干渉稿の強弱は２つのフォトダイオード７ａ，７ｂで逆位相なので、両者の差信号をとると、図２（ｂ）に示すように干渉稿の部分のみを取り出すことができる。このとき干渉稿の振幅は信号光Ｓの光子数ｎ１ と参照光Ｌの光子数ｎ０ の積の平方根の２倍、すなわち$2\sqrt{n1}\sqrt{n0}$である。なお、信号光Ｓと参照孔Ｌの振幅は強度の平方根、つまり$\sqrt{n1}$と$\sqrt{n0}$であり、フォトダイオード７ａとフォトダイオード７ｂとの差の最大値は$\{(\sqrt{n1}+\sqrt{n0})^2/2-(\sqrt{n1}-\sqrt{n0})^2/2\}=2\sqrt{n1}\sqrt{n0}$となる。

【００２３】

さらに上述したのは多数回の平均値であり、１回ごとの差信号の測定結果には信号光Ｓの量子揺らぎにより標準偏差$\sqrt{n0}$の揺らぎが存在する。

図３は信号光の量子状態の揺らぎを考慮した場合の受信者側の測定信号の模式図であり、（ａ）は光路差が０度の場合、（ｂ）は光路差が９０度（λ／４）の場合、（ｃ）は光路差が１８０度（λ／２）の場合、（ｄ）は光路差が２７０度（３λ／４）の場合であり、それぞれ横軸は差信号の大きさを示し、縦軸はその信号が検出される確率を示す。

なおλは光の波長を示し、横軸は差信号を$2\sqrt{n0}$で割って規格化してある。

【００２４】

図３（ａ）に示すように、信号光Ｓと参照光Ｌとの相対的な光路差が０度の場合、信号光Ｓが平均光子数１のコヒーレント状態の場合に得られる差信号の頻度

分布は平均値が１で、標準偏差が０．５のガウス分布となる。図３の（ｂ）～（ｄ）の場合は、それぞれ０，－１，０となる。

したがって、量子暗号を実行するためには、受信者は１回ごとの測定について光路差が０度であったのか、あるいは１８０度であったのかを差信号の測定結果から判断することが可能になる。つまり、図３の（ａ）と（ｃ）とを区別すればよいので、しきい値Ｘ－、Ｘ＋を定めて、差信号がＸ＋以上であれば０度、Ｘ－以下であれば１８０度と判断することができる。

【００２５】

このようにＸ－とＸ＋とを設定することにより実効的な検出効率と誤り率を自由に設定できる。例えば図３のｎ１ ＝１の場合に、Ｘ－＝Ｘ＋＝０とすると、光路差が０度のときに０度と判断する確率（実効的な検出確率）は、ガウス分布を｛（平均値）－（標準偏差の２倍）｝から無限大まで積分すればよいので、９７．７％となる。逆に光路差が１８０度であるのに０度と判断してしまう確率（誤り率）はガウス分布を｛（平均値）＋（標準偏差の２倍）｝から無限大まで積分したものなので２．２８％となる。またＸ－＝－０．５、Ｘ＋＝０．５とすると、同様の計算により実効的な検出確率が８４．１％まで低下するが、誤り率が０．１３％と非常に小さくなり、従来より優れた性能が得られる。

【００２６】

図４は第１の実施形態の測定結果の例であり、（ａ）は５０００回測定したときの差信号の頻度分布図であり、横軸は実際の測定電圧である。（ｂ）は（ａ）のような測定を３０回行って得たデータから計算機トモグラフィーにより求めた信号光のウィグナー分布関数の図である。ウィグナー分布関数は信号光の量子状態の表現方法の一つであり、ウィグナー分布関数が得られたことは信号光の量子状態の測定が実際に可能であることを示している。

本実施形態の測定では５０００個の光パルスに対して差信号の電圧値を測定し頻度分布を求めたものであり、図４（ａ）に示すように頻度分布はガウス関数に従っている。なお、図４（ａ）の横軸は実際の測定電圧であるので、分布の幅を図３の場合と直接比較するには、増幅器の利得と参照光の強度を使って補正する必要がある。

このような補正をすれば、測定された分布の幅（差信号の揺らぎの大きさ）は量子揺らぎで予測される幅と一致することが確かめられる。

【００２７】

図４（ｂ）は光路差を変化させながら５０００回の測定を３０組、計１５万パルス分のデータから求めたウィグナー分布関数である。

このように本発明の第１の実施形態では、光路差を変化させながら測定を行うことにより、信号光の量子力学的な状態の測定が可能である。ウィグナー分布関数は信号光について理論上知りうる全ての情報を含んでいるので、盗聴者の存在による信号光の変化を、より簡単に見いだすことが可能になる。

【００２８】

次に量子暗号の手順について説明する。

図５は本発明による量子暗号の手順を示す表であり、左欄の１は送信者の位相変調、２は受信者の位相変調、３は送信者と受信者の位相変調の合計、４は受信者の測定結果、５は受信者が自分の加えた位相変調を送信者に公衆回線で伝え、送信者が位相変調の合計が、０度又は１８０度のとき○を、９０度又は２７０度のとき×を受信者に通知したこと、６は受信者が＋にビット１を、－にビット０を、○になった場合につき当てはめ秘密鍵としたこと、７は送信者が自分の位相変調が、０度又は９０度のときはビット１を、１８０度又は２７０度のときはビット０を当てはめ秘密鍵としたことを示す。なお、ここでは簡単のため誤り率を０とする。

【００２９】

まず送信者は図１中の鏡３を制御することにより、０度、９０度、１８０度及び２７０度の位相の変化をランダムに信号光に加える（図５の左欄１）。一方受信者は鏡５により、０度又は９０度のランダムな位相変化を参照光に加える（同左欄２）。このとき合計の光路差は送信者と受信者の位相変調の差となる（同左欄３）。

さらに受信者は測定結果に対して上述したＸ－、Ｘ＋の設定に従い、差信号がＸ－以下であれば「－」を、Ｘ＋以上であれば「＋」を割り当てる（同左欄４）。このとき左欄３が０度のときは必ず＋、１８０度のときは－、９０度と２７０

度のときは＋と－とが等確率で現れる（同左欄４）。

【００３０】

次に受信者はビットが０か１であった場合について、０度と９０度のどちらの位相変調を加えたかを例えば公衆回線を通じて送信者に連絡する（同左欄５）。

送信者は合計の光路差が０度か１８０度であったものについて、秘密鍵として採用することを受信者に連絡する。すなわち、送信者は位相変調の合計が０度又は１８０度のとき○を、９０度又は２７０度のとき×を受信者に通知する（同左欄５）。

受信者は＋にビット１を、－にビット０を、○となった場合につき当てはめ秘密鍵とする（同左欄６）。

そして送信者は自分の加えた位相変調が０度と９０度のものはビット１を、１８０度と２７０度のものはビット０を当てはめ秘密鍵とする（同左欄７）。

図５で示すように、このようにして生成された秘密鍵は送信者と受信者とで必ず一致する。

【００３１】

次に盗聴を知る方法を説明する。

量子的な測定は対象に必ず影響を及ぼすという原理により、第三者による盗聴の試みは伝送信号に必ず変化を与えるので、送信者と受信者とに気づかれずに第三者がこの秘密鍵を知ることは不可能である。

具体的な信号の変化は盗聴者がどのような手段をとるかに依存する。例えば盗聴者がいったん信号光を遮って情報を読み取り、受信者に信号を再送するという手段をとった場合、盗聴者の情報の読み取りに上述した受信者と同じ測定を行うとすると、誤った位相変調のときには（送信者の位相変調との合計が９０度や２７０度のとき）送信者の位相変調を知ることができず、受信者に正しい信号を再送することができない。

【００３２】

一般に互いに９０度離れた振幅成分の両方の情報を得ることは不確定性関係により不可能であるので、盗聴者がどのような手段で情報を読み取るとしても正しい情報は得られず、必ず誤り率の増加となって現れる。すなわち、送信者と受信

者の秘密鍵が一致しない。例えば盗聴者が信号光をいったん遮って再送するという手段をとった場合は、不適切な位相変調を行う確率１／２と誤った信号を再送する確率１／２を掛け合わせた確率１／４で、送信者と受信者との秘密鍵が一致しない。

したがって、秘密鍵の一部を照らし合わせることにより盗聴者の存在を検出することができる。

【００３３】

また信号光の一部を分離して測定して情報を部分的に得て、分離したことによる損失を増幅によって補うという盗聴手段の場合、従来の量子暗号では低い量子効率と相まって検出が困難であったが、本発明の場合ではウィグナー分布関数の変化となって現れるので受信者は直ぐ気付くことになる。これは増幅過程が量子揺らぎの増減を必ず伴うので、図４（ａ）のような測定結果において分散の増減となって現れ、ウィグナー分布関数もピーク値のまわりの分布が全体的に太くなったり非対称となり、また盗聴者が確定的な情報を得た場合のみ増幅する盗聴手段をとった場合には、ピーク値をとるＸ1 、Ｘ2 の値も変化することになるからである。

【００３４】

次に第２の実施形態について説明する。

この第２の実施形態は、伝送路として１本の光ファイバーを用いることを想定しており、上述した第１の実施形態のままでは困難である長距離の量子暗号を可能にするための実装である。そのために参照光と信号光とを時間及び偏光状態で分離し、同一の経路を伝送させるようにしたものであり、受信者の信号処理や量子暗号の手順は上述した第１の実施形態と同様である。

ただし、送信者と受信者との位相変調に量子暗号の手続に加え、別に予め定めた位相変調を与えることにより、光路差の安定性の改善と量子状態のモニターのための操作を加えている。

【００３５】

安定性の改善は、予め定めた位相変調の場合に予測される差信号と実際に測定される差信号との比較により行う。量子状態のモニターは一様に変化する位相変

調を予め定めた位相変調として与えることにより実行できる。

【００３６】

図６は第２の実施形態の量子暗号装置の模式図である。

図６を参照すると、第２の実施形態は送信者側に、直線偏光のパルス光を発生するレーザー光源２１と、このパルス光を２つに分割するビームスプリッター２２と、一方の経路の光、これを信号光として、信号光Ｓの偏光を９０度回転する半波長板２４と、吸収媒質により信号光Ｓの強度を弱くする光減衰器２５と、信号光Ｓの位相を変化させる位相変調器２６と、他方の経路の光、これを参照光Ｌとして、この参照光Ｌと信号光Ｓとを同一光軸上に戻す偏光ビームスプリッター２３とを備え、参照光Ｌと信号光Ｓとを光ファイバー２７に入射するようになっている。このとき信号光Ｓと参照光Ｌとは互いに偏光が直交しており、かつ、時間的に離れた状態となっている。なお、図６中の１８，１９は鏡を示す。

【００３７】

光ファイバー２７の出力側には光ファイバー伝送中の偏光の乱れを補正する偏光素子２８が設けられている。本発明では参照光Ｌの強度が強いので、この参照光Ｌを用いて補正を行っている。

受信者側には、信号光Ｓと参照光Ｌとを分離する偏光ビームスプリッター２９と、先ほどとは逆に距離的に短い経路を通し途中で位相変化を信号光Ｓに与える位相変調器３０と、長い経路を通して参照光Ｌの偏光を９０度回転する半波長板３１と、参照光Ｌと信号光Ｓとを時間的及び偏光方向も一致させる無偏光ビームスプリッター３２とを備え、この無偏光ビームスプリッター３２からの参照光Ｌと信号光Ｓとをそれぞれフォトダイオード３３ａ、３３ｂにより電気信号に変化し、その差信号を増幅器及び電圧測定器３５で増幅し、電圧を測定するようになっている。なお、図６中の３８，３９は鏡を示す。

【００３８】

このような構成により、信号光Ｓと参照光Ｌとが異なる経路を進むのは送信者と受信者側の短い距離だけで、大部分の伝送路は同一の経路を進むので、２つの光の相対的な光路差の変動を小さくすることができる。

【００３９】